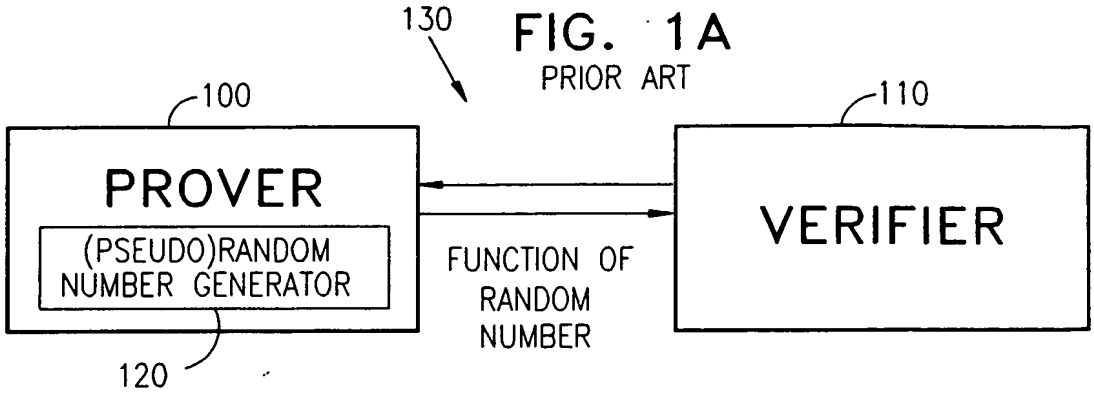


FIG. 1A
PRIOR ART

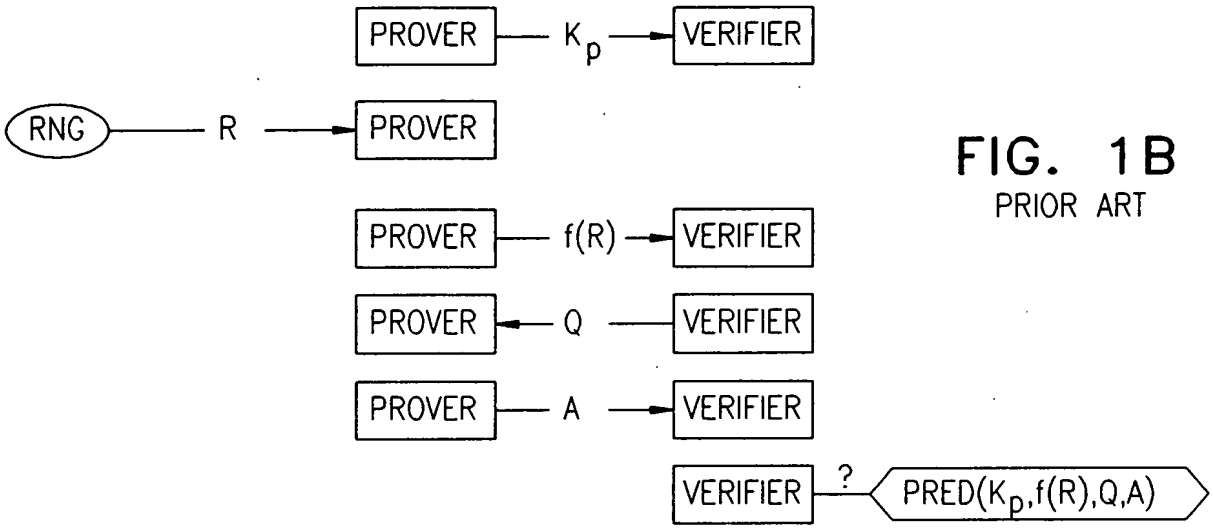


FIG. 1B
PRIOR ART

FIG. 1C
PRIOR ART

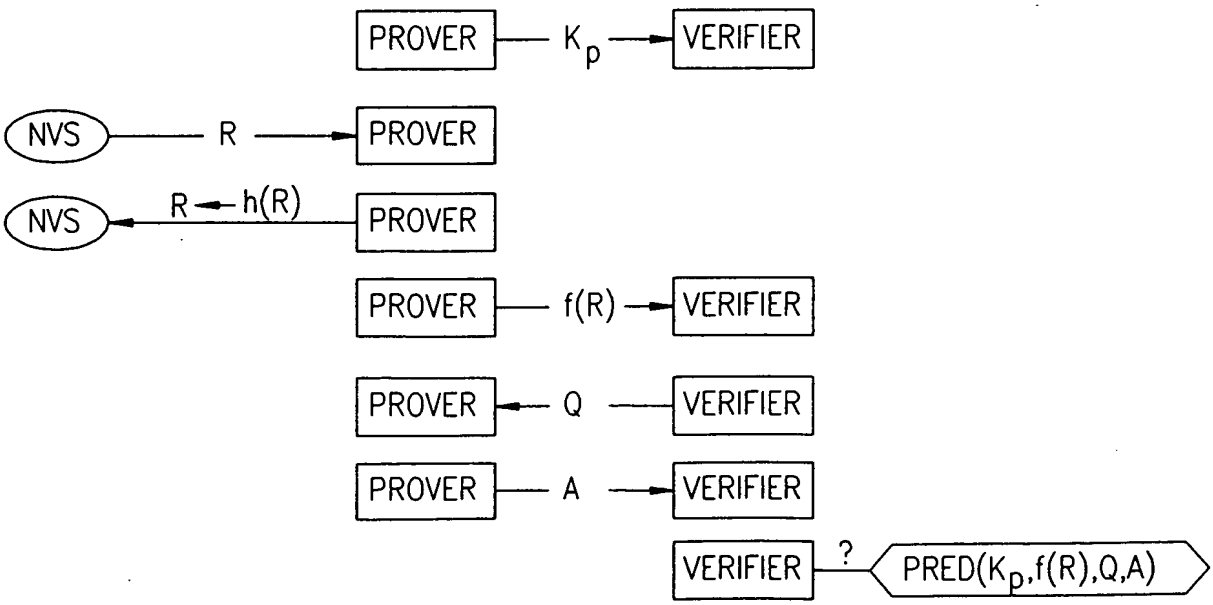


FIG. 2

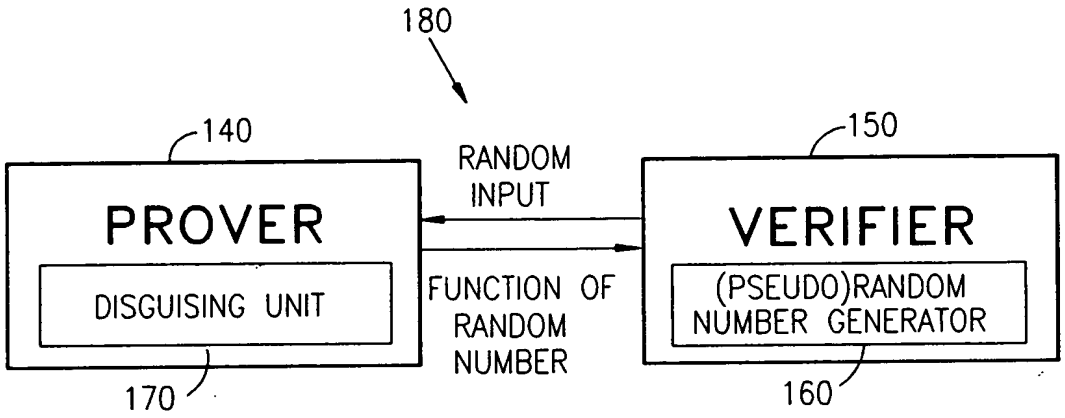

180
140
150
PROVER
DISGUISING UNIT
170
RANDOM INPUT
FUNCTION OF RANDOM NUMBER
VERIFIER
(PSEUDO)RANDOM NUMBER GENERATOR
160

FIG. 3

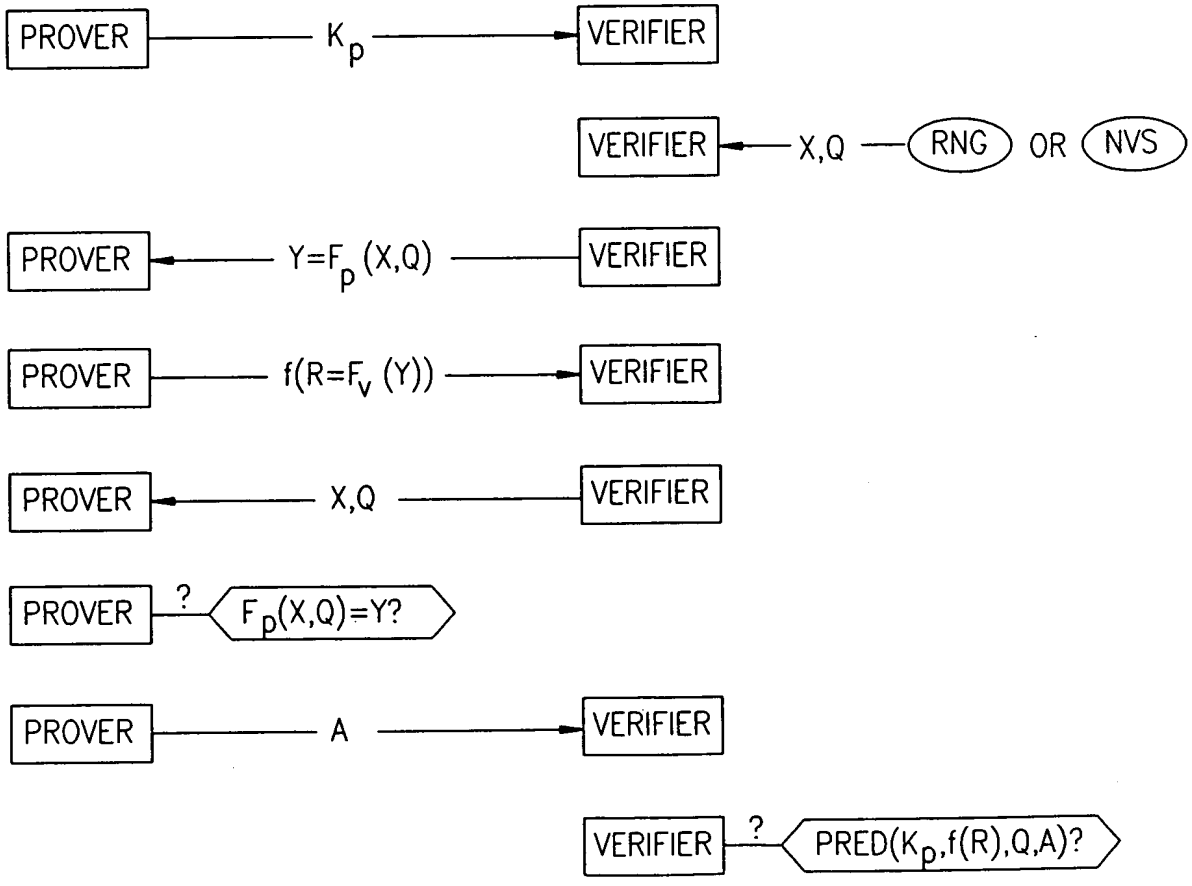

PROVER
K_p
VERIFIER
VERIFIER
X,Q
RNG
OR
NVS
PROVER
$Y=F_p(X,Q)$
VERIFIER
PROVER
$f(R=F_v(Y))$
VERIFIER
PROVER
X,Q
VERIFIER
PROVER
?
$F_p(X,Q)=Y?$
PROVER
A
VERIFIER
VERIFIER
?
$PRED(K_p,f(R),Q,A)?$

FIG. 4A

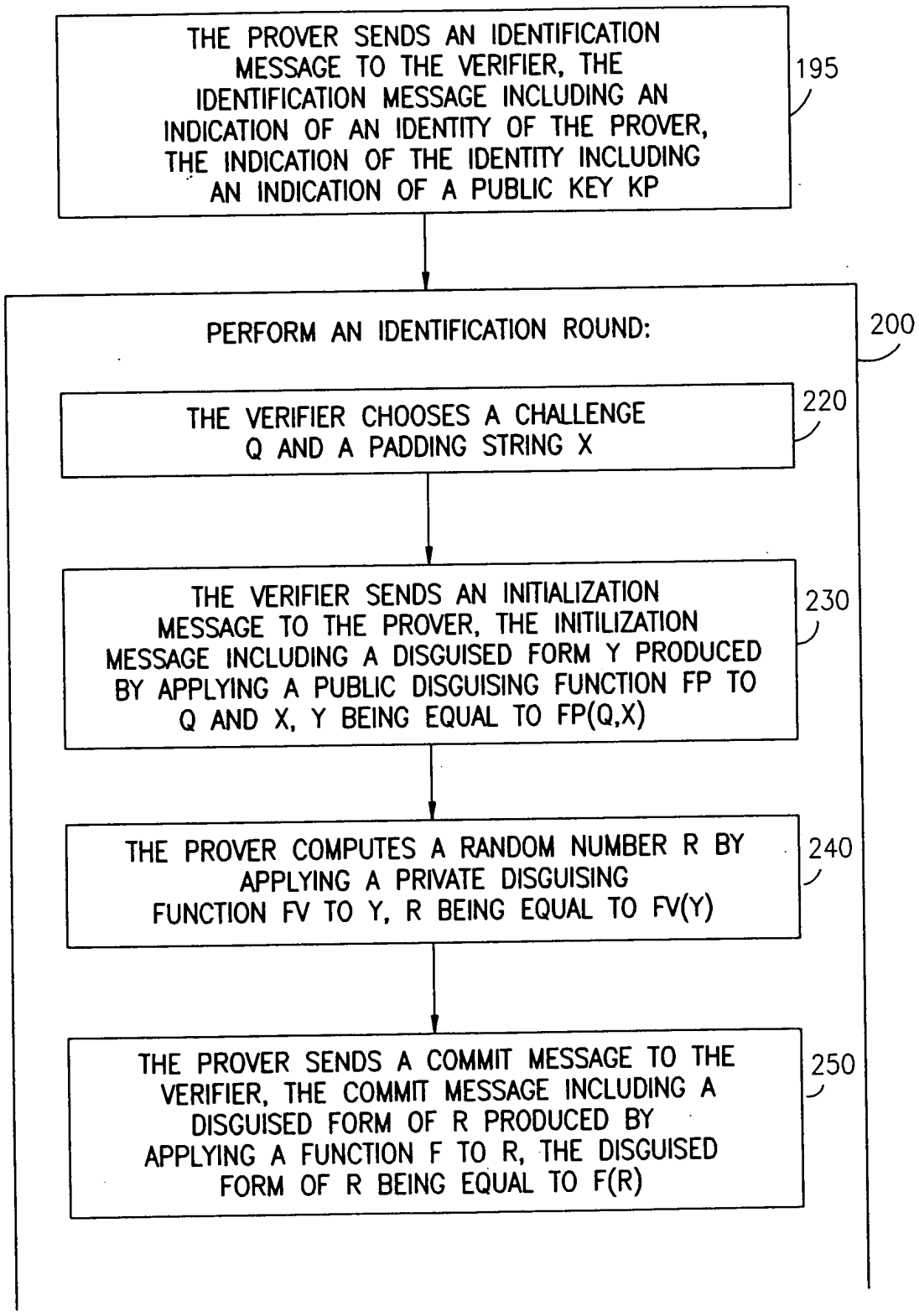
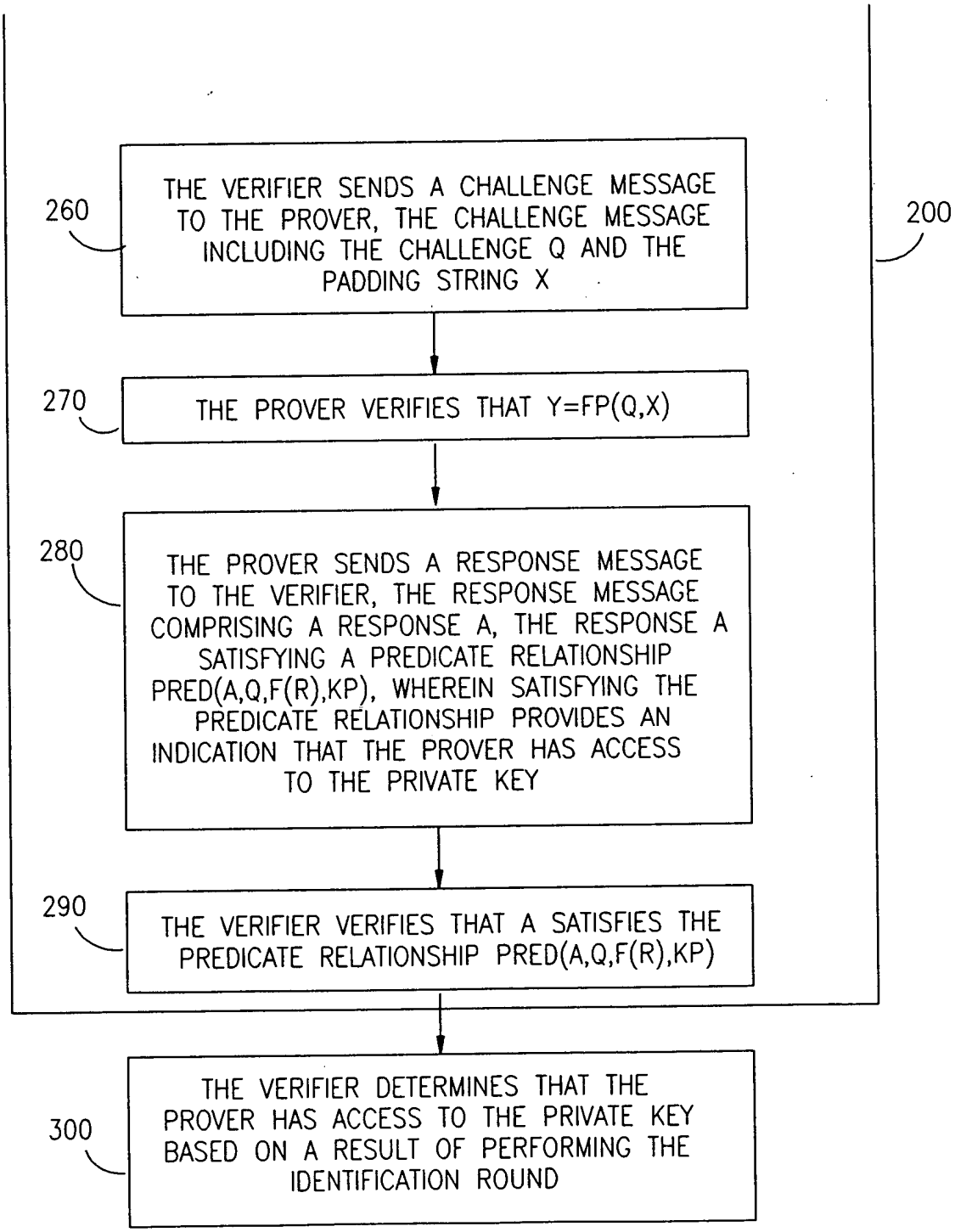

THE PROVER SENDS AN IDENTIFICATION MESSAGE TO THE VERIFIER, THE IDENTIFICATION MESSAGE INCLUDING AN INDICATION OF AN IDENTITY OF THE PROVER, THE INDICATION OF THE IDENTITY INCLUDING AN INDICATION OF A PUBLIC KEY KP
195
PERFORM AN IDENTIFICATION ROUND:
200
THE VERIFIER CHOOSES A CHALLENGE Q AND A PADDING STRING X
220
THE VERIFIER SENDS AN INITIALIZATION MESSAGE TO THE PROVER, THE INITILIZATION MESSAGE INCLUDING A DISGUISED FORM Y PRODUCED BY APPLYING A PUBLIC DISGUISING FUNCTION FP TO Q AND X, Y BEING EQUAL TO FP(Q,X)
230
THE PROVER COMPUTES A RANDOM NUMBER R BY APPLYING A PRIVATE DISGUISING FUNCTION FV TO Y, R BEING EQUAL TO FV(Y)
240
THE PROVER SENDS A COMMIT MESSAGE TO THE VERIFIER, THE COMMIT MESSAGE INCLUDING A DISGUISED FORM OF R PRODUCED BY APPLYING A FUNCTION F TO R, THE DISGUISED FORM OF R BEING EQUAL TO F(R)
250

FIG. 4B


200
260
THE VERIFIER SENDS A CHALLENGE MESSAGE TO THE PROVER, THE CHALLENGE MESSAGE INCLUDING THE CHALLENGE Q AND THE PADDING STRING X
270
THE PROVER VERIFIES THAT Y=FP(Q,X)
280
THE PROVER SENDS A RESPONSE MESSAGE TO THE VERIFIER, THE RESPONSE MESSAGE COMPRISING A RESPONSE A, THE RESPONSE A SATISFYING A PREDICATE RELATIONSHIP PRED(A,Q,F(R),KP), WHEREIN SATISFYING THE PREDICATE RELATIONSHIP PROVIDES AN INDICATION THAT THE PROVER HAS ACCESS TO THE PRIVATE KEY
290
THE VERIFIER VERIFIES THAT A SATISFIES THE PREDICATE RELATIONSHIP PRED(A,Q,F(R),KP)
300
THE VERIFIER DETERMINES THAT THE PROVER HAS ACCESS TO THE PRIVATE KEY BASED ON A RESULT OF PERFORMING THE IDENTIFICATION ROUND